newswit.com

6 February 2013
Source: http://www.newswit.com

Executives urged to improve information security levels as risks set to rise – PwC

Businesses must ensure that they have robust information security safeguards in place to protect their operations and attract more clients as IT-related risks continue to rise, according to a PwC survey. PwC warns that business leaders globally are far too optimistic about the strength of their security frameworks.

PwC's 10th annual survey on the Global State of Information Security® 2013, which featured interviews with more than 9,300 top-ranking executives from 128 countries, found that 68% of executives are confident of their organisation's information security precautions. Another 42% even viewed their organisation as a 'front-runner', meaning they have an effective strategy in place and are proactive in implementing industry-leading standards in information security strategy and execution.

However, the survey found that only 8% actually qualify as true information security leaders. PwC defines 'leaders' as companies that have a chief information security officer (CISO) or equivalent in place; have an overall information security strategy; have measured and reviewed the effectiveness of their security in the last year; and understand exactly what types of security events have occurred.

Vilaiporn Taweelappontong, Consulting Partner at PwC Thailand, said that the rise in global security incidents, diminished budgets and degrading security programmes are key challenges that have left many businesses around the globe to deal with security risks that are neither well understood nor consistently addressed.

"The reality is that many top executives are over-confident about the strength of their information security effectiveness," Vilaiporn said. "That leaves businesses open to fraud and reduces their attractiveness to potential clients as the number of IT security incidents increases."

Worryingly, the survey also found that fewer than half of the respondents (45%) expect an increase in their information security budgets in the next 12 months, despite a rise in the number of respondents reporting 50 or more security-related incidents (13%). The drop was down from 51% and 52% in 2011 and 2010 respectively. Economic conditions were rated as the most essential factor that shaped security budget—cited by 46% of respondents—but the most frequently cited answers didn't concern the business value of good information security.

“Of course, people feel the pinch in tough economic times, but crooks don’t take holidays. Tying budgets too closely to the economy is a risky way to set security priorities,” Vilaiporn said.

In fact, the survey also showed that many companies actually decreased their deployment of basic information security and anti-piracy tools. Among the categories taking a hit were malicious code detection tools for spyware and adware, down to 71% after topping out at 84% in 2008, and intrusion detection tools, once in use by nearly two-thirds of respondents and now used by just over half.

“What most businesses don’t realise is that they must embrace a new way of thinking in which information security is no longer just a means to protect data but an opportunity to create value for the organisation. Crucial things like security strategies and spending really have to be well-aligned with business goals,” Vilaiporn added.

Asia to lead 2013 security spending

Looking at security spending growth by region, however, the survey showed that years of investment pay off as Asia now leads the world in security practices and performance. About 60% of Asian businesses expect to boost information security spending over the next 12 months, ahead of their US and Europe counterparts. Although the number was down from 74% in 2011, it was still among the highest for any region. As for keeping up with new challenges, Asia rates highly for mobile security initiatives and cloud security strategy.

“For many years, Asia has been firing up its investment in security. Again this year’s result, despite a drop from the year before, showed just how far the region has advanced its capabilities,” said Vilaiporn.

“Confidence in information security runs high in Asia, and at least some of this confidence is justified by the extent to which strategy, technology, and processes are in place. What we also found most interesting is that Asian organisations are the second most likely to incorporate security into major projects from the start, and are more likely than their peers in other regions to base security spending on factors like business continuity and disaster recovery, rather than other external factors,” she explained.

Despite Asia’s lead in practices and performance, North America ties Asia for the lead in cloud security strategy and leads in mobile and social media security. Responses from North American firms indicated that they are the least likely to outsource security functions and are the best at staying on plan when it comes to IT projects, the survey showed.

In today’s world of ‘big data’, the survey found that most organisations are keeping looser tabs on their data today than in past years. Fewer than 35% of respondents said they had an accurate inventory of employee and customer personal data, and only 31% reported they had an accurate accounting of locations and jurisdictions of stored data.

Big data defines a collection of both structured and unstructured data sets so large and complex that it becomes difficult to process using on-hand database management tools or traditional data processing applications. It has become a hot topic for most businesses over the past few years. Organisations have always had to deal with

large amounts of data and needed to invest in hardware and software capabilities in order to gain competitive advantage.

As mobile devices, social media, and the cloud become commonplace both inside the enterprise and out, the survey found that the adoption of technology is moving faster than security.

According to the report, 88% of consumers use a mobile device for both personal and work purposes, yet only 45% of companies have a security strategy to address personal devices in the workplace, and just 37% have malware protection for mobile devices.

“Security models of the past decade are no longer sufficient. Businesses around the world, including Thailand, should see information security as a valuable investment that protects both the business reputation and their bottom line. Businesses have no choice but to improve the strength of their IT security if they are to enter the Asean Economic Community in the next few years on a strong footing and with the capabilities to compete on a regional scale,” Vilaiporn concluded.